

**1.0 PURPOSE AND SCOPE:**

- 1.1 The company collects and processes personal information or personal data, relating to its employees, contractors and visitors, in order to manage the working relationship, as well as to allow the business to meet statutory and non-statutory obligations.
- 1.2 Lignacite Ltd is fully committed to ensuring the security and protection of the personal information that it holds and processes, and to provide a compliant and consistent approach to data protection.
- 1.3 The company is committed to safeguarding the personal information under its remit and in maintaining a data protection system that is effective and fit for purpose.
- 1.4 The purpose of this policy is to outline arrangements the company has put in place to meet its requirements under the General Data Protection Regulations (GDPR) and the Data Protection Act 1998.
- 1.5 This policy applies to all employees at both the Brandon and Nazeing sites.

**2.0 POLICY:**

- 2.1 There are eight core data protection principles outlined in the regulations, which the company and all of its employees, without exception, must adhere to at all times.

These principles are defined as follows:

- (a) Information will be processed fairly and lawfully and will not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data.

These conditions require that either the employee has given consent to the processing of the personal data, or that the processing of the data is necessary for the various purposes outlined in the legislation.

Sensitive personal data will only be processed with the explicit consent of the employee and will consist of information relating to:

- Race or ethnic origin
- Political opinions or trade union memberships
- Religious or other beliefs
- Physical or mental health
- Sexual preference
- Criminal offences, including both committed and alleged

- (b) Personal data will be obtained for one or more specified and lawful purposes only and not processed in a manner incompatible with those purposes.

- (c) Personal data processed will be relevant and proportionate. The company will review information stored in personal files at least annually to ensure that they do not contain a backlog of out-of-date information (as per the retention schedule), and to check if there are additional business reasons for storing the information.

It is the responsibility of all employees to ensure that their line manager is notified of any relevant changes to their personal data (e.g., change of address or next of kin).

Section: Corporate		Reference No.: CO007	
Page 1 of 4	Issue Date:07/07/2022	Issue No.: 001	Author: Marvyn Candler

The business cannot be held responsible for any errors unless they have been notified of the relevant change.

- (d) Personal data will not be stored for any longer than is necessary. Retention periods for different types of data will vary depending on legal, operational and financial requirements. The business maintains a retention schedule in the integrated management system to fully outline required minimum retention periods.

Any personal data which the company no longer needs to retain will be securely destroyed.

- (e) All personal data will be processed in accordance with the requirements outlined in the General Data Protection Regulations (GDPR) and the Data Protection Act 1998.
- (f) Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data. Hard copies of personal information remain confidential and will be stored in locked cabinets only. Access to these files will be restricted to authorised personnel only.

Where information is processed and stored digitally on servers, cloud systems or personal computers, personal data will be kept confidential and protected by way of password protection, encryption or coding. Systems are designed to ensure that only authorised persons have access to the personal data.

- (g) Personal data will not be transferred to any country outside of the UK or European Union, unless that country ensures an adequate level of protection for the processing of personal data.

- 2.2 The need for the business to retain personal data about its employees will be fully detailed on the contract of employment. By signing the contract of employment, employees are fully consenting to this data being processed by the company.

The personal data the company retains will include information for payroll, human resources and business continuity purposes.

All employees are required to agree to the business processing their personal data as a condition of their employment. As part of this agreement all employees are required to fully cooperate with the company with regards to any reasonable request for personal data made to them.

Examples of such requests would include copy of driving licence, passport, as well personal contact details, next of kin and date of birth

- 2.3 The business will hold sensitive personal data about its employees, where necessary. By signing the contract of employment, employees are giving their explicit consent to the company holding this information

Examples of such information would include information required for equal opportunities monitoring, as well as medical and health surveillance records.

- 2.4 All employees have the right, on request, to receive copies of all personal information that the business holds about them, including their personnel file. They also have the right to demand that any inaccurate data be corrected or removed.

- 2.5 Employees also, have the right, upon request, to:

Section: Corporate	Reference No.: CO007		
Page 2 of 4	Issue Date:07/07/2022	Issue No.: 001	Author: Marvyn Candler

- Be informed by the company whether personal data about them is being processed and for what purpose
- Be provided with a description of the data and any recipients to whom it may be disclosed
- Have any personal data about them communicated to them, in an understandable form, along with any information related to the source of the data
- Be informed of the logic involved in any computerised decision making

**2.6** Upon request, the company will provide its employees with a statement regarding any personal data held about them. This statement will list all the different types of personal data the company holds about you and the reasons for holding it.

**2.7** Any requests for copies of personal data, must be put in writing to the relevant line manager or department head.

**2.8** Any complaints regarding any personal data being held, should be put in writing to the relevant line manager or department head.

Where employees believe that the company has not complied with their data protection rights, have the right to report the complaint directly to the Information Commissioner's Office (ICO). The ICO is the UK authority for data protection issues.

### **3.0 OBLIGATIONS IN RELATION TO PERSONAL DATA:**

**3.1** Where employees, as part of their duties and responsibilities, collect personal information about employees or other people, the terms of this policy must be complied with fully.

This includes ensuring that the information is only processed in accordance with the purpose for which it is held, is kept secure and not kept for any longer than is necessary.

**3.2** All employees collecting personal data as part of their roles and responsibilities, must adhere to the following at all times:

- Do not disclose confidential personal information to anyone except the data subject, without explicit written permission of the data subject. In particular it should not be:
  - given to someone from the same family
  - passed to any other unauthorised third party
  - placed on the company's website
  - posted on the internet in any form

unless explicit prior written permission has been given by the data subject.

- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identify of the data subject and the legitimacy of the request.
- Where the company has encrypted data with passwords or security keys, these must not be shared with any unauthorised person or third-party organisation at any time.
- Personal information should only be transferred digitally (e.g. email or instant messaging) if a secure network is in place.

Section: Corporate		Reference No.: CO007	
Page 3 of 4	Issue Date:07/07/2022	Issue No.: 001	Author: Marvyn Candler

- Any requests for personal information about another employee should be forwarded on to the Company Secretary, through the relevant line manager or department head.

Signed:.....*C. de Lotbiniere*.....  
GAJ de Lotbiniere, Chairman

Date:.....15/7/22.....

Section: Corporate		Reference No.: CO007	
Page 4 of 4	Issue Date:07/07/2022	Issue No.: 001	Author: Marvyn Candler